

Configuring NetFlow Data Export

This chapter describes how to configure NetFlow Data Export (NDE) on the Catalyst 5000 and 2926G series switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference* for your switch.

This chapter consists of these sections:

- Understanding How NetFlow Data Export Works on page 43-1
- Software and Hardware Requirements on page 43-3
- Default NetFlow Data Export Configuration on page 43-3
- Configuring NetFlow Data Export on page 43-3

Understanding How NetFlow Data Export Works

These sections describe how NDE works:

- Understanding NDE and Integrated MLS Management on page 43-1
- MLS Data Collection on page 43-2
- Using NDE Filters on page 43-3

Understanding NDE and Integrated MLS Management

You can use NDE to monitor all MLS intersubnet traffic through the NFFC or NFFC II and the RSM (or externally attached router). NDE complements the embedded Remote Monitoring (RMON) capabilities on the switch that allow you to see all port traffic.

Note For information on configuring MLS, see Chapter 42, “Configuring Multilayer Switching.”

Integrated MLS management includes products, management utilities, and partner applications designed to gather flow statistics, export the statistics, collect and perform data reduction on the exported statistics, and forward them to applications for traffic monitoring, planning, and

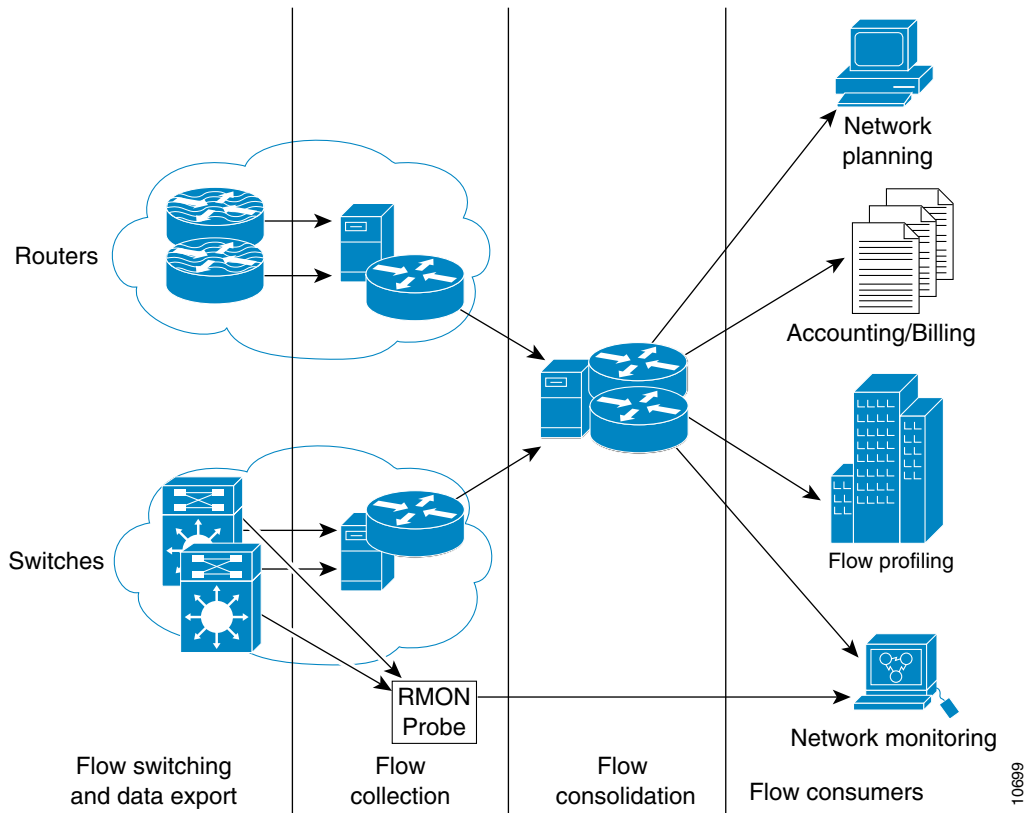
accounting. Flow collectors, such as the Cisco SwitchProbe and NetFlow FlowCollector, gather and classify flows. This flow information is then aggregated and fed to applications such as TrafficDirector, NetSys, or NetFlow Analyzer.

We recommend the Catalyst 5000 series Network Analysis Module (WS-X5380) or the Cisco SwitchProbe device as the flow collector for MLS. The Network Analysis Module provides extended RMON support and can analyze Ethernet VLAN traffic exported from the NFFC or NFFC II. For more information about the Network Analysis Module, see Chapter 33, “Configuring the Network Analysis Module.” The SwitchProbe device supports the two versions of data (Versions 1 and 7) exported from the RSM and NFFC or NFFC II using NDE. SwitchProbe proxies the data to RMON2 for viewing from the TrafficDirector application. Support is also included for the RMON2 Management Information Base (MIB) group. Refer to the *SwitchProbe Installation and Configuration Guide* for information about SwitchProbe.

MLS Data Collection

An external data collector gathers flow entries from the MLS cache of one or more switches or Cisco routers. The switch or router transmits data to the flow collector by grouping flow entries for expired flows from its MLS cache into a User Datagram Protocol (UDP) datagram, which consists of a header and a series of flow entries. Figure 43-1 illustrates the NDE process.

Figure 43-1 Integrated MLS Management



Using NDE Filters

By default, *all* expired flows are exported until you specify a filter. After specifying a filter, only expired and purged flows matching the specified filter criteria are exported. Filter values are stored in nonvolatile RAM (NVRAM) and are not cleared when NDE is disabled.

If the flow mask is destination-ip mode and the NDE filter contains a filter on both source and destination, only the destination filter is effective. For example, in the filter specified in the following display if the flow mask is in destination-ip mode, all flows with destination address 9.1.2.15 are exported. The source filter for host 10.1.2.15 is not effective (it is ignored).

```
Console> (enable) set mls nde flow destination 9.1.2.15/32 source 10.1.2.15/32
Netflow data export: destination filter set to 9.1.2.15/32
Netflow data export: source filter set to 10.1.2.15/32
Console> (enable)
```

Software and Hardware Requirements

NDE requires these software and hardware versions:

- Supervisor engine software—Software release 4.1(1) or later
- Cisco IOS router software—IOS release 11.3(2)WA4(4) or later
- Catalyst 2926G series switch or a Catalyst 5000 series switch with Supervisor Engine III, III FSX, or III FLX module with a NetFlow Feature Card (NFFC) or NFFC II
- Route Switch Module (RSM) or Cisco 7500, 7200, 4500, or 4700 series router
- RMON data collector (such as the Catalyst 5000 series Network Analysis Module)

Default NetFlow Data Export Configuration

Table 43-1 shows the default NDE configuration.

Table 43-1 Default NetFlow Data Export Configuration

Feature	Default Value
NDE	Disabled
NDE data collector address and UDP port	None specified ¹
NDE filters	None configured

¹ With a Network Analysis Module installed, you do not need to specify an external data collector address.

Configuring NetFlow Data Export

These sections describe how to configure NDE:

- Specifying a NetFlow Data Export Address on page 43-4
- Specifying a NetFlow Data Export Collector on page 43-5
- Enabling NetFlow Data Export on page 43-5
- Specifying a Destination Host Filter on page 43-6
- Specifying a Destination and Source Subnet Filter on page 43-6
- Specifying a Destination TCP/UDP Port Filter on page 43-6

- Specifying a Source Host and Destination TCP/UDP Port Filter on page 43-6
- Specifying a Protocol Filter on page 43-7
- Specifying Protocols for Statistics Collection on page 43-7
- Removing Protocols for Statistics Collection on page 43-7
- Clearing an NDE Flow Filter on page 43-8
- Disabling NetFlow Data Export on page 43-8
- Removing the NetFlow Data Export Address on page 43-8
- Displaying the NDE Configuration on page 43-9

Specifying a NetFlow Data Export Address

The MLS-RP and the MLS-SE use the NDE IP address when sending MLS statistics to a data collection application. You must configure the IP address on the MLS-RP so the data collection application can aggregate export data from both the MLS-RP and the MLS-SE for the same flow.

If you do not specify an NDE IP address for the MLS-RP, the MLS-RP automatically selects the IP address of one of its interfaces and uses that IP address as its NDE IP address and its MLS IP address.

If you manually specify an NDE IP address for the MLS-RP, the MLS-RP uses this IP address as its MLS IP address (as shown in the output of the **show mls rp** command), replacing the one that was automatically selected.

After specifying the NDE IP address for the MLS-RP, enter the **show mls rp** command and note the “mls ip address.” You must add this address to the included MLS router list on the switch. For information on how to add a router to the list of routers participating in MLS, see the “Specifying Routers to Participate in MLS” section on page 42-20.



Caution When you enable MLS on the router, the MLS-RP automatically selects one of its interfaces as the NDE IP address. If you later enable NDE and you specify a different NDE IP address from the automatically selected address, you must include the new MLS IP address in the list of routers participating in MLS on the switch, as described in the “Specifying Routers to Participate in MLS” section on page 42-20.

To specify an NDE IP address for the MLS-RP, perform this task in global configuration mode:

Task	Command
Specify the NDE IP address for the router.	Router(config)# mls rp nde-address [ip_addr]

This example shows how to specify an NDE IP address on the MLS-RP:

```
Router(config)#mls rp nde-address 170.170.2.1
Router(config)#
```

Specifying a NetFlow Data Export Collector

Before enabling NDE for the first time, you must specify an NDE collector and UDP port to receive the exported statistics. The collector address and UDP port number are saved in NVRAM and are preserved if NDE is disabled and reenabled or if the switch is power cycled.

Note If you are using the NetFlow FlowCollector application for data collection, verify that the UDP port number you specify is the same port number shown in the FlowCollector's `nfconfig.file`. This file is located at `/opt/csconfc/config/nfconfig.file` in the FlowCollector application.

Note If you have a Catalyst 5000 series Network Analysis Module (WS-X5380) installed, you do not have to specify the NDE collector IP address and UDP port. The Network Analysis Module receives NDE statistics from the NFFC or NFFC II automatically. Proceed to the "Enabling NetFlow Data Export" section on page 43-5 to enable NDE on the switch.

To specify a NetFlow data export collector, perform this task in privileged mode:

Task	Command
Specify an NDE collector and UDP port.	set mls nde <i>[collector_ip]</i> <i>[udp_port_number]</i>

This example shows how to specify a NetFlow data export collector:

```
Console> (enable) set mls nde Stargate 9996
Netflow data export not enabled.
Netflow data export to port 9996 on 172.20.15.1 (Stargate)
Console> (enable)
```

Enabling NetFlow Data Export

To enable NDE, perform this task in privileged mode:

Task	Command
Enable NDE on the switch.	set mls nde enable

This example shows how to enable NDE on the switch:

```
Console> (enable) set mls nde enable
Netflow data export enabled.
Netflow data export to port 9996 on 172.20.15.1 (Stargate)
Console> (enable)
```

If you attempt to enable NDE without first specifying a collector, you see this display:

```
Console> (enable) set mls nde enable
Please set host name and UDP port number with 'set mls nde <collector_ip>
<udp_port_number>'.
Console> (enable)
```

Specifying a Destination Host Filter

To specify a destination host filter, perform this task in privileged mode:

Task	Command
Specify a destination host filter for an NDE flow.	set mls nde flow destination <i>[ip_addr_spec]</i>

This example shows how to set a destination host filter so that only expired flows to host 171.69.194.140 are exported:

```
Console> (enable) set mls nde flow destination 171.69.194.140
Netflow data export: destination filter set to 171.69.194.140/32
Console> (enable)
```

Specifying a Destination and Source Subnet Filter

To specify a destination and source subnet filter, perform this task in privileged mode:

Task	Command
Specify a destination and source subnet filter for an NDE flow.	set mls nde flow destination <i>[ip_addr_spec]</i> source <i>[ip_addr_spec]</i>

This example shows how to specify a destination and source subnet filter so that only expired flows to subnet 171.69.194.0 from subnet 171.69.173.0 are exported (assuming the flow mask is set to source-destination-ip):

```
Console> (enable) set mls nde flow destination 171.69.194.140/24 source 171.69.173.5/24
Netflow data export: destination filter set to 171.69.194.0/24
Netflow data export: source filter set to 171.69.173.0/24
Console> (enable)
```

Specifying a Destination TCP/UDP Port Filter

To specify a destination TCP/UDP port filter, perform this task in privileged mode:

Task	Command
Specify a destination TCP/UDP port filter for an NDE flow.	set mls nde flow dst prt <i>[port_number]</i>

This example shows how to specify a destination TCP/UDP port filter so that only expired flows to destination port 23 are exported (assuming the flow mask is set to ip-flow):

```
Console> (enable) set mls nde flow dst_port 23
Netflow data export: destination port filter set to 23.
Console> (enable)
```

Specifying a Source Host and Destination TCP/UDP Port Filter

To specify a source host and destination TCP/UDP port filter, perform this task in privileged mode:

Task	Command
Specify a source host and destination TCP/UDP port filter for an NDE flow.	set mls nde flow source <i>[ip_addr_spec]</i> dst prt <i>[port_number]</i>

This example shows how to specify a source host and destination TCP/UDP port filter so that only expired flows from host 171.69.194.140 to destination port 23 are exported (assuming the flow mask is set to ip-flow):

```
Console> (enable) set mls nde flow source 171.69.194.140 dst_port 23
Netflow data export: destination port filter set to 23
Netflow data export: source filter set to 171.69.194.140/32
Console> (enable)
```

Specifying a Protocol Filter

To specify a protocol filter, perform this task in privileged mode:

Task	Command
Specify a protocol filter for an NDE flow.	set mls nde flow protocol <i>protocol</i>

This example shows how to specify a protocol filter so that only expired flows from protocol 17 are exported:

```
Console> (enable) set mls nde flow protocol 17
Netflow Data Export filter successfully set.
Protocol filter is 17
Console> (enable)
```

Specifying Protocols for Statistics Collection

You can use the **set mls statistics protocol *protocol port*** command to specify up to 64 different protocols for which to collect statistics to be exported using NDE. The *protocol* argument can be **tcp**, **udp**, **icmp**, or a decimal number for other protocol families. The *port* argument specifies the protocol port.

To specify protocols for statistics collection, perform this task in privileged mode:

Task	Command
Specify protocols for statistics collection.	set mls statistics protocol <i>protocol port</i>

This example shows how to specify a protocol for statistics collection:

```
Console> (enable) set mls statistics protocol 17 1934
Protocol 17 port 1934 is added to protocol statistics list.
Console> (enable)
```

Removing Protocols for Statistics Collection

You can use the **clear mls statistics protocol {*protocol port* | **all**}** command to specify up to 64 different protocols for which to collect statistics to be exported using NDE. The *protocol* argument can be **tcp**, **udp**, **icmp**, or a decimal number for other protocol families. The *port* argument specifies the protocol port. Use the **all** keyword to remove all protocols for statistics collection.

To remove protocols for statistics collection, perform this task in privileged mode:

Task	Command
Remove protocols for statistics collection.	clear mls statistics protocol {<i>protocol port</i> all}

This example shows how to remove a protocol for statistics collection:

```
Console> (enable) clear mls statistics protocol 17 1934  
Protocol 17 port 1934 cleared from protocol statistics list.  
Console> (enable)
```

Clearing an NDE Flow Filter

To clear the NDE flow filter and reset the filter to the default (all flows exported), perform this task in privileged mode:

Task	Command
Clear the NDE flow filter.	clear mls nde flow

This example shows how to clear the NDE flow filter so that all flows are exported:

```
Console> (enable) clear mls nde flow  
Netflow data export filter cleared.  
Console> (enable)
```

Disabling NetFlow Data Export

Note If NDE is enabled and you disable MLS, you lose the statistics for existing cache entries—they are not exported.

To disable NDE, perform this task in privileged mode:

Task	Command
Disable NDE on the switch.	set mls nde disable

This example shows how to disable NDE on the switch:

```
Console> (enable) set mls nde disable  
Netflow data export disabled.  
Console> (enable)
```

Removing the NetFlow Data Export Address

To remove the NDE IP address from the MLS-RP, perform this task in global configuration mode:

Task	Command
Remove the NDE IP address for the router.	Router(config)#no mls rp nde-address [ip_addr]

This example shows how to remove the NDE IP addresses on the MLS-RP:

```
Router(config)#no mls rp nde-address 170.170.2.1  
Router(config)#
```

Displaying the NDE Configuration

To display the NDE configuration, perform this task in privileged mode:

Task	Command
Show the NDE configuration on the switch.	show mls nde

This example shows how to display the NDE configuration on the switch:

```
Console> (enable) show mls nde
Netflow Data Export enabled
Netflow Data Export configured for port 1098 on host 172.20.15.1
Source filter is 171.69.194.140/255.255.255.0
Destination port filter is 23
Total packets exported = 26784
Console> (enable)
```

